

Forum:[Hack Forums](#)

Thread: [OpenSSL upgrading connection to TLS](#)

Byte™ - April 15, 2018, 2:30 pm

All I want to do is connect to an SMTP server, talk to it and then request it to perform a handshake mid connection. How would I go about doing that? I believe it has something to do with creating a SSL_BIO and then pushing it onto original connection bio.

Oversimplified example of what I am trying to do.

EDIT

The code represents what I did to promote the bio to a secure connection.

Code #include <openssl/bio.h>

#include <openssl/ssl.h>

#include <openssl/err.h>

#include <vector>

int main(){

```
std::string HelloString = "ehlo 127.0.0.1\r\n";
std::vector<char> buffer(5000);
```

```
//Connect to gmail SMTP server
```

```
BIO * bio = BIO_new_connect("smtp.gmail.com:587");
```

```
BIO_do_connect(bio);
```

```
//Read server hello
```

```
BIO_read(bio, buffer.data(), buffer.size());
```

```
//write client hello
```

```
BIO_write(bio, HelloString.c_str(), HelloString.length());
```

```
//read server ack and commands
```

```
BIO_read(bio, buffer.data(), buffer.size());
```

```
//Tell the server I want to upgrade the connection
```

```
BIO_write(bio, "STARTTLS\r\n", 10);
```

```
//Upgrade the connection some how
```

```
//Edited Version
```

```
SSL_CTX * ctx = SSL_CTX_new(SSLv23_client_method());
```

```
BIO * ssl_bio = BIO_new_ssl(ctx, 1);
```

```
BIO * ssl_chain = BIO_push(ssl_bio, bio);
```

```
BIO_do_handshake(ssl_chain);
```

```
//Completed - Start sending data as TLS
```

```
return 0;
```

```
}
```

Edit

I found the answer to my problem by reading some OpenSSL source code, what you can do is create a SSL_BIO with BIO_NEW_SSL and then append the BIO to the SSL_BIO and then call bio_do_handshake with the SSL_BIO.